

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - -X

IN THE MATTER OF AN APPLICATION FOR
A SEARCH WARRANT FOR:

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

THE PREMISES KNOWN AND DESCRIBED AS
ELECTRONIC MAIL ADDRESS

A) dimpledond456@aol.com,
B) kingkon1851@aol.com,
C) nikkinikki4real@aol.com,
D) reekal029@hotmail.com,
E) nflowers2010@gmail.com,
F) blakrepublikin@gmail.com,
G) joelchaudry@yahoo.com,
H) lisa.saint213@gmail.com,
I) f.joe14@ymail.com.

- - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

STACEY SULLIVAN, being duly sworn, deposes and states
that he is a Special Agent with the Federal Bureau of
Investigation, duly appointed according to law and acting as
such.

Upon information and belief, there is probable cause to
believe that there is located in THE PREMISES KNOWN AND DESCRIBED
AS ELECTRONIC MAIL ADDRESSES "A) DIMPLEDON456@AOL.COM, B)
KINGKON1851@AOL.COM, C) NIKKINIKKI4REAL@AOL.COM, D)
REEKA1029@HOTMAIL.COM, E) NFLOWERS2010@GMAIL.COM, F)
BLAKREPUBLIKINC@GMAIL.COM, G) JOELCHAUDRY@YAHOO.COM, H)
LISA.SAINT213@GMAIL.COM, I) F.JOE14@YMAIL.COM (the "EMAIL
PREMISES") subscriber/profile information, email transmission
information, subject headings, to/from information, folders and

email content (including all of the foregoing for deleted messages), as described more fully in Attachment E, which constitute evidence, fruits and instrumentalities of identification fraud, aggravated identity theft, access device fraud, and bank fraud, in violation of Title 18, United States Code, Sections 1028, 1028A, 1029 and 1341.

The source of your deponent's information and the grounds for her belief are as follows:¹

1. I have been a Special Agent with the Federal Bureau of Investigation for two years. During my tenure with the FBI, I have been involved in numerous fraud investigations.

2. I have personally participated in the investigation of the offense referred to above, and from my personal participation in this investigation and from reports made to me by other law enforcement officers, I am familiar with the facts and circumstances of this investigation. Because this Affidavit is being submitted for the limited purpose of seeking search warrants, I have not set forth each and every fact learned during the course of this investigation, but simply those facts which I believe are necessary to establish probable cause to support the issuance of search warrants of the EMAIL PREMISES. Except where

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

otherwise noted, all conversations described in this Affidavit are set forth in part and in substance only.

I. PROBABLE CAUSE

3. From late 2010 to the present, FBI agents have been investigating a group of individuals located primarily in Brooklyn, who are participating in a scheme to fraudulently obtain credit card numbers and manufacture and use credit cards. Specifically, the scheme involves purchasing stolen credit card numbers through ICQ chats, printing those credit card numbers onto real credit card blanks, and using those credit cards to make purchases in retail stores.

4. In late 2010, a confidential human source ("CHS") informed the FBI that an individual named KWAN MILLER and several other individuals, all located in Brooklyn, were fraudulently printing credit cards. The CHS indicated that MILLER obtained stolen credit card numbers through ICQ chats with individuals overseas. MILLER and his associates then used these credit card numbers to print credit cards using specialized credit card printing equipment. The printed credit cards were then provided to other individuals who purchase goods, which are then sold for profit. The CHS also indicated that MILLER and his associates also print false identification documents.

5. The CHS also had consensual access to computer systems used by MILLER during the course of this scheme. FBI agents

received two external hard drives containing information from MILLER's computers from the CHS, which were consensually copied. The hard drives contain lists of credit card numbers. I have confirmed that many of those credit card numbers are real credit card numbers associated with the accounts of real people in New Jersey, Pennsylvania, Florida, Texas and California, among others. The credit cards found on the hard drives were issued by numerous different financial institutions in the United States, including Bank of America, Wells Fargo, USAA, and Chase Manhattan. The lists of credit cards numbers also include credit card numbers that were issued by foreign banks. Some of these credit card numbers correspond to accounts that remain open today, while some correspond to accounts at which fraud has been reported. Based on the results of responses to grand jury subpoenas, I have determined that at least \$100,000 of fraudulent charges have been made using these credit card numbers. The issuing banks have suffered losses of over \$10,000 related to this fraudulent scheme.

6. The hard drives also contained templates of driver's licenses for various states. They also contained passport-type photographs for a number of individuals.

7. The CHS also indicated in late 2010 that one e-mail address used by MILLER was dimpledon456@aol.com. The CHS also provided the ICQ account number of MILLER. Subpoena responses

have confirmed that the address dimpled456@aol.com was used to register that ICQ address on September 5, 2009 and remains registered to MILLER's ICQ address. The hard drives also contained several e-mails from the dimpled456@aol.com e-mail address, including an e-mail dated November 16, 2009 from joelchaudry@yahoo.com to dimpled45@aol.com which stated "yo, send me the bin." Based on my investigation, I am aware that a BIN is a bank identification number, which consists of the first six digits of a credit card number. An e-mail dated November 16, 2009 from dimpled45@aol.com to joelchaudry@yahoo.com, responded "531001/374190."

8. Subpoena responses have also shown that MILLER has bought numerous specialty printers designed to print credit cards and identification cards between 2004 and January 2011. In addition, MILLER has purchased numerous supplies for these printers. The most recent purchases were made using a credit card in the name KWAN MILLER and shipped to the address identified by a database search as MILLER's home address. A representative of the company that distributes these specialty printers indicated that on or about March 15, 2011, MILLER called the company and asked for a sheet indicating the current prices for printers. MILLER requested that the pricing sheets be e-mailed to him at kingkon1851@aol.com.

9. On April 8, 2011, the Honorable Andrew L. Carter issued a

search warrant for the email accounts dimpled45@aol.com and kingkon1851@aol.com. On June 1, 2011, the Honorable Robert M. Levy issued a search warrant for the email accounts dimpled45@aol.com, kingkon1851@aol.com, nikkinikki4real@aol.com, reeka1029@hotmail.com, nflowers2010@gmail.com, blakrepublikin@gmail.com, and joelchaudry@yahoo.com. On June 11, 2011, the Honorable Viktor V. Pohorelsky issued a search warrant amending riders to the June 1, 2011 search warrant. I have subsequently received emails pursuant to those search warrants, among which were the following emails which establish probable cause to search the EMAIL PREMISES:

a. On January 3, 2010, dimpled456@aol.com sent an email to nikkinikki4real@aol.com with an attachment entitled "2010 work.txt." The attachment is a text file that contains dozens of numbers I have identified to be credit card numbers. In addition, the attachment contains "track 1" and "track 2" information, which is additional information related to the credit card number that would be necessary to encode that credit card number on a fraudulent credit card blank.

b. On November 9, 2010, lisa.saint213@gmail.com sent an email to nflowers2010@gmail.com that included a list of numbers I have identified to be credit card numbers.

c. On January 30, 2011, kingkon1851@aol.com sent

an email to reekal029@hotmail.com, which listed dozens of numbers I have identified to be credit card numbers. In addition, the email contains "track 1" and "track 2" information.

d. On February 28, 2011, kingkon1851@aol.com sent an email to nflowers2010@gmail.com with an attachment entitled "final.txt." The attachment is a text file that contains dozens of numbers I have identified to be credit card numbers. In addition, the attachment contains "track 1" and "track 2" information.

e. On March 27, 2011, blakrepublikinc@gmail.com sent reekal029@hotmail.com and kingkon1851@aol.com an email message that consisted of a forwarded telephone multimedia message ("MMS"). The MMS consisted of a photograph of a passport-style picture depicting a black male. The photograph is consistent with those used on identification documents. The CHS identified above also indicated that blakrepublikinc@gmail.com was an e-mail address used by KWAN MILLER.

f. On April 22, 2011, reekal029@hotmail.com sent an email to kingkon851@aol.com which listed dozens of numbers which I have identified to be credit card numbers. In addition, listed after each number was a description such as "CENTURION amex unknown unknown various EU" or "BLUE FOR BUSINESS amex unknown unknown various EU".

g. On June 2, 2011, f.joe14@ymail.com sent

reeka1029@hotmail.com an email message containing a listing of numbers and names which I have identified to be credit card numbers. On June 3, 2011, reeka1029@aol.com forwarded that message to kingkon1851@aol.com

II. TECHNICAL BACKGROUND

10. The SUBJECT EMAIL PREMISES are email accounts hosted by the service providers AOL, Inc., Windows Live Hotmail, Google, Inc. and Yahoo! Inc. (hereinafter, the "email providers").

11. Based on my training and experience, I know the following about AOL, Inc. ("AOL"):

a. AOL provides email service to customers utilizing its services. Subscribers obtain an email account by registering with AOL. AOL requests subscribers to provide basic information, such as name, ZIP code and other personal/biographical information. However, AOL does not verify the information provided.

b. AOL maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information.

c. Subscribers to AOL may access their accounts on servers maintained and/or owned by AOL from any computer connected to the Internet located anywhere in the world.

d. Any email that is sent to a AOL subscriber is stored in the subscriber's "mail box" on AOL's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by AOL. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on AOL's servers indefinitely.

e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to AOL's servers, and then transmitted to its end destination. AOL users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the AOL server, the email can remain on the system indefinitely. The sender can delete the stored email message thereby eliminating it from the email box maintained at AOL, but that message will remain in the recipient's email box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

f. An AOL subscriber can store files, including emails and image files, on servers maintained and/or owned by AOL.

g. Emails and image files stored on an AOL server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store emails

and/or other files on the AOL server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the AOL server.

h. A subscriber of AOL can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by the email provider.

12. Based on my training and experience, I have learned the following about Windows Live Hotmail ("Hotmail"):

a. Hotmail provides e-mail service to customers utilizing its services. Subscribers obtain an e-mail account by registering with Hotmail. Hotmail requests subscribers to provide basic information, such as name, zip code and other personal/biographical information. However, Hotmail does not verify the information provided;

b. Hotmail maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information;

c. Subscribers to Hotmail may access their

accounts on servers maintained and/or owned by Hotmail from any computer connected to the Internet located anywhere in the world;

d. Any e-mail that is sent to a Hotmail subscriber is stored in the subscriber's "mail box" on Hotmail's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by Hotmail. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on Hotmail's servers indefinitely;

e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Hotmail's servers, and then transmitted to its end destination. Hotmail users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Hotmail server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at Hotmail, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

f. A Hotmail subscriber can store files, including e-mails and image files, on servers maintained and/or owned by Hotmail; and

g. E-mails and image files stored on a Hotmail server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and/or other files on the Hotmail server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Hotmail server.

h. A subscriber of Hotmail can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by the email provider.

13. Based on my training and experience, I have learned the following about Google, Inc. ("Gmail"):

a. Gmail provides e-mail service to customers utilizing its services. Subscribers obtain an e-mail account by registering with Gmail. Gmail requests subscribers to provide basic information, such as name and other personal/biographical information. However, Gmail does not verify the information provided;

b. Gmail maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access

information, e-mail transaction information, and account application information;

c. Subscribers to Gmail may access their accounts on servers maintained and/or owned by Gmail from any computer connected to the Internet located anywhere in the world;

d. Any e-mail that is sent to a Gmail subscriber is stored in the subscriber's "mail box" on Gmail's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by Gmail. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on Gmail's servers indefinitely;

e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Gmail's servers, and then transmitted to its end destination. Gmail users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Gmail server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at Gmail, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

f. A Gmail subscriber can store files, including

e-mails and image files, on servers maintained and/or owned by Gmail; and

g. E-mails and image files stored on a Gmail server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and/or other files on the Gmail server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Gmail server.

h. A subscriber of Gmail can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by the email provider.

14. Based on my training and experience, I know the following about Yahoo! Inc. ("Yahoo!"):

a. Yahoo! provides email service to customers utilizing its services. Subscribers obtain an email account by registering with Yahoo!. Yahoo! requests subscribers to provide basic information, such as name, ZIP code and other personal/biographical information. However, Yahoo! does not verify the information provided.

b. Yahoo! maintains electronic records pertaining

to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information.

c. Subscribers to Yahoo! may access their accounts on servers maintained and/or owned by Yahoo! from any computer connected to the Internet located anywhere in the world.

d. Any email that is sent to a Yahoo! subscriber is stored in the subscriber's "mail box" on Yahoo!'s servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Yahoo!. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on Yahoo!'s servers indefinitely.

e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Yahoo!'s servers, and then transmitted to its end destination. Yahoo! users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Yahoo! server, the email can remain on the system indefinitely. The sender can delete the stored email message thereby eliminating it from the email box maintained at Yahoo!, but that message will remain in the recipient's email box unless

the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

f. A Yahoo! subscriber can store files, including emails and image files, on servers maintained and/or owned by Yahoo!.

g. Emails and image files stored on a Yahoo! server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Yahoo! server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Yahoo! server.

h. A subscriber of Yahoo! can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by the email provider.

i. Yahoo! offers email addresses ending in both yahoo.com and ymail.com.

15. In my experience, subscribers do not routinely copy emails stored in their online account in order to store the emails on a home computer or other location, although it is possible to do so. This is particularly true when they access

their email account through the web, or if they do not wish to maintain particular emails or files in their residence.

16. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the email provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

17. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well

records of any actions taken by the provider or user as a result of the communications.

18. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files.

III. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

19. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the email provider to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment E. Upon receipt of the information described in Section I of Attachment E, government-authorized persons will review that information to locate the items described in Section II of Attachment E.

IV. CONCLUSION

20. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of the email provider there exists evidence of crimes. Accordingly, a search warrant is requested.

21. This Court has jurisdiction to issue the requested

warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

22. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

23. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly through online forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

24. It is respectfully requested that this Court issue an order preventing the disclosure of this search warrant by service providers. Disclosure of this search warrant by service providers may have significant and negative impact on the continuing investigation and severely jeopardize its effectiveness. If this search warrant is disclosed to the users of the email addresses being searched, those individuals, who are the targets of the investigation, are likely to change e-mail addresses and otherwise take measures to further conceal their illegal activities from law enforcement.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS ELECTRONIC MAIL ADDRESSES "A) DIMPLEDON456@AOL.COM, B) KINGKON1851@AOL.COM, C) NIKKINIKKI4REAL@AOL.COM, D) REEKA1029@HOTMAIL.COM, E) NFLOWERS2010@GMAIL.COM, F) BLAKREPUBLIKINC@GMAIL.COM, G) JOELCHAUDRY@YAHOO.COM, H) LISA.SAINT213@GMAIL.COM, I) F.JOE14@YMAIL.COM."

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

Stacey Sullivan
Special Agent
Federal Bureau of Investigation

Sworn to before me this
__th day of ___, 2011

UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with DIMPLEDON456@AOL.COM, KINGKON1851@AOL.COM, and NIKKINIKKI4REAL@AOL.COM that is stored at premises owned, maintained, controlled, or operated by AOL, Inc., a company headquartered in New York, New York.

ATTACHMENT B

Property to Be Searched

This warrant applies to information associated with REEKA1029@HOTMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Windows Live Hotmail, a company headquartered in Mountain View, California.

ATTACHMENT C

Property to Be Searched

This warrant applies to information associated with NFLOWERS2010@GMAIL.COM, BLAKREPUBLIKINC@GMAIL.COM, and LISA.SAINT213@GMAIL.COM, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered in Mountain View, California.

ATTACHMENT D

Property to Be Searched

This warrant applies to information associated with JOELCHAUDRY@YAHOO.COM and F.JOE14@YMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Yahoo! Inc., a company headquartered in Sunnyvale, California.

ATTACHMENT E

Particular Things to be Seized

I. Information to be disclosed

To the extent that the information described in Attachments A to D is within the possession, custody, or control of the service provider identified in Attachments A to D, each service provider is required to disclose the following information to the government for each account or identifier listed in Attachments A to D:

- a. The contents of all emails stored in the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- d. All records pertaining to communications between the service provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information obtained from the service provider will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1028, 1028A, 1209 and 1341, since January 2010,

including, for each account or identifier listed on Attachments A to D, information pertaining to the following matters:

- a. Trafficking in stolen credit card numbers, production of counterfeit credit cards, use of counterfeit credit cards or stolen credit card numbers, and production of false identification documents.
- b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.